FORM PTO-1390
(REV 11-2000)

U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY 'S DOCKET NUMBER
148/259

U.S APPLICATION NO (If known, see 37 CFR 1 5
09/763103

INTERNATIONAL APPLICATION NO. PCT/GB99/02672	INTERNATIONAL FILING DATE August 12, 1999	PRIORITY DATE CLAIMED August 20, 1998

TITLE OF INVENTION
IMPROVEMENTS IN AND RELATING TO DATA COMMUNICATION

APPLICANT(S) FOR DO/EO/US
ABDULHAYOGLU, Melih

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☒ is attached hereto (required only if not communicated by the International Bureau).
   b. ☐ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☐ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☐ Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). - UNSIGNED
10. ☐ An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☒ Other items or information: Amended Claims

U.S. APPLICATION NO (if known, see 37 CFR 1.5) 09/763103	INTERNATIONAL APPLICATION NO PCT/GB99/02672	ATTORNEY'S DOCKET NUMBER 148/259

	CALCULATIONS	PTO USE ONLY
21. ☒ The following fees are submitted: **BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):** Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO .... **$1000.00** International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO .... **$860.00** International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO .... **$710.00** International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) .... **$690.00** International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**	$ 860.00	
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 130.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than □ 20 ☒ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	$	
Total claims	25 - 20 =	5	x **$18.00**	$ 90.00	
Independent claims	3 - 3 =	0	x **$80.00**	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$270.00**	$	

TOTAL OF ABOVE CALCULATIONS =	$ 1080.00	
☒ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2. +	$	
SUBTOTAL =	$ 540.00	
Processing fee of **$130.00** for furnishing the English translation later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).	$	
TOTAL NATIONAL FEE =	$ 540.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +	$	
TOTAL FEES ENCLOSED =	$ 540.00	
	Amount to be refunded:	$
	charged:	$

a. ☒ A check in the amount of $ 540.00 to cover the above fees is enclosed.

b. □ Please charge my Deposit Account No. __________ in the amount of $ ________ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 01-0265. A duplicate copy of this sheet is enclosed.

d. □ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

ADAMS, SCHWARTZ & EVANS, P.A.
2180 Two First Union Center
Charlotte, NC 28282
(704) 375-9249

23638
PATENT TRADEMARK OFFICE

SIGNATURE

Jeffrey J. Schwartz
NAME

37,532
REGISTRATION NUMBER

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	ABDULHAYOGLU, Melih
INTERNATIONAL APPLICATION NO.:	PCT/GB99/02672
INTERNATIONAL FILING DATE:	August 12, 1999
FOR:	IMPROVEMENTS IN AND RELATING TO DATA COMMUNICATION

BOX PCT
Assistant Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Sir:

After the assignment of a serial number and prior to the initial examination of the above-identified patent application, please make the following amendments:

IN THE SPECIFICATION:

Amend the specification by inserting after the title, but before the first sentence on page 1:

--This application is a national stage application, according to Chapter II of the Patent Cooperation Treaty.--

APPLICANT: ABDULHAYOGLU, Melih

INTERNATIONAL APPLICATION NO.: PCT/GB99/02672

IN THE CLAIMS:

Cancel original claims 1 - 25.

Add claims 1 - 25 as attached and entitled "Amended Claims."

REMARKS

It is believed that this application is now in condition for allowance. Such action at an early date is respectfully requested.

Respectfully submitted,

Jeffrey J. Schwartz
Reg. No. 37,532

Jeffrey J. Schwartz
ADAMS, SCHWARTZ & EVANS, P.A.
2180 First Union Plaza
301 S. Tryon Street
Charlotte, NC 28282
TEL: (704) 375-9249
FAX: (704) 375-0729
E-Mail: jjs@adamspat.com
File No. 148/259

Amended Claims

1. A method for password enhancing, which method comprises the steps of entering a user password and irreversibly encrypting the user password.

2. A method according to claim 1, in which the encryption comprises a hash operation.

3. A method according to claim 1, in which the method comprises the additional step of using an encrypted first stored key (NEPKEY) to encrypt the irreversibly encrypted user password (HASH).

4. A method according to claim 3, in which the first stored key is encrypted by a public key encryption algorithm.

5. A method according to claim 3, in which the method comprises the additional step of decrypting an encrypted second stored key (UPEK) using the decrypted first stored key (NEPKEY).

6. A method according to claim 5, in which the second stored key is encrypted by a reversible algorithm.

7. A method according to claim 5, in which the result (HASH) of the irreversibly encrypted user password is encrypted using the second stored key (UPEK) as an encryption key.

8. A data access method comprising the steps of producing an enhanced password according to claim 1, comparing the enhanced password with a password associated with the data, and permitting access to the data only if the enhanced password and the data password correspond.

9. A computer program for carrying out the method of claim 8.

10. A carrier comprising a program according to claim 9.

11. A data communication system comprising an input device for generating a plurality of input signals available from a set of input signals and a character generator configured to receive an input signal and generate an output signal comprising a plurality of signals from the set of input signals in which the output signal is different from the signal input to the character generator.

12. A data communication system according to claim 11, in which the output signal is of a different length to the signal input to the character generator.

13. A data communication system according to claim 12, in which the output signal is longer than the signal input to the character generator.

14. A data communication system according to claim 11, in which the system further comprises means for comparing the output signal with a stored password.

15. A data communication system according to claim 14, in which the comparison means further comprises means for outputting a signal dependent upon the correspondence of the output signal with the stored password.

16. A data communication system according to claim 11, in which the input device comprises a keyboard.

17. A data communication system according to claim 16, in which the set of available input signals comprises all or part of the character set of the keyboard.

18. A data communication system according to claim 11, in which the system comprises a first input and a second input in which the character generator receives signals from the first input and does not receive signals from the second input.

19. A data communication system according to claim 18, in which the first input is a local input device such as a keyboard or microphone and the second input is a remote based input device typically providing signals via a modem connection.

20. A data communication system according to claim 19, in which the input signal comprises or corresponds to one of the set of input signals.

21. A data communication system according to claim 20, in which the set of input signals comprises alphanumeric characters.

22. A digital computer comprising a data communication system according to claim 11.

23. A data communication method comprising receiving an input signal available from a set of input signals, generating an output signal comprising a plurality of signals from the set of available input signals, in which the output signal is different from the input signal.

24. A method according to claim 23, in which the method further comprises the step of repeating the operation for a plurality of input signals.

25. A method according to claim 23, in which the output signals vary in length one from the other.

IMPROVEMENTS IN AND RELATING TO DATA COMMUNICATION

Field of the Invention

The present invention relates to data communication devices and methods, and to programs for executing such methods and carriers therefor.

Background to the Invention

With the growth of computer networks, including the internet, local area networks, wide area networks and intranets, additional problems have been created in relation to computer security. In particular, the possibilities for unauthorised remote access into a computer (sometimes referred to as "hacking") have been increased.

Hackers seeking unauthorised access have developed various forms of software to assist in these attacks, including those that make multiple attempts to gain access through password controlled systems. Typically such software will try various permutations of possible passwords until the correct one is found. This can either be a "dictionary" attack, restricted to known words, or a "brute force" attack which tries all permutations. For this reason, amongst others, many systems require passwords of a minimum length, but as these have to be memorised by a user only a certain minimum length is practicable. Thus, many password lengths fall in the range of 4-8 characters and are often everyday words for case of recollection. This makes a software-assisted attack on the system a real risk to any password protected function or data.

It is an aim of preferred embodiments of the present invention to obviate or overcome at least one disadvantage encountered in relation to the prior art, whether referred to herein or otherwise.

Summary of the Invention

According to the present invention in a first aspect, there is provided a method for password enhancing, which method comprises the steps of entering a user password and irreversibly encrypting the user password.

Preferred embodiments of the present invention provide for more secure password handling, by enhancing the password.

Suitably, the encryption comprises a hash operation.

Suitably, the method comprises the additional step of using an encrypted first stored key (NEPKEY) to encrypt the irreversibly encrypted user password (HASH). Suitably, the first stored key is encrypted by a public key encryption algorithm.

Suitably, the method comprises the additional step of decrypting an encrypted second stored key (UPEK) using the decrypted first stored key (NEPKEY). Suitably, the second stored key is encrypted by a reversible algorithm.

Suitably, the result (HASH) of the irreversibly encrypted user password is encrypted using the second stored key (UPEK) as an encryption key.

According to the present invention in a second aspect, there is provided a data access method comprising the steps of producing an enhanced password according to the first aspect of the present invention, comparing the enhanced password with a password associated with the data, and permitting access to the data only if the enhanced password and the data password correspond.

The data to be accessed may be any type, including a file, an application, a data record etc.

According to the present invention in a third aspect there is provided a computer program for carrying out the method of the second aspect of the present invention.

According to the present invention in a fourth aspect, there is provided a carrier comprising a program according to the third aspect of the invention.

According to the present invention in a fifth aspect, there is provided a data communication system comprising an input device for generating a plurality of input signals available from a set of input signals and a character generator configured to receive an input signal and generate an output signal comprising a plurality of signals from the set of input signals in which the output signal is different from the signal input to the character generator.

Suitably, the output signal is of a different length to the signal input to the character generator. More suitably, the output signal is longer than the signal input to the character generator.

Suitably, the system further comprises means for comparing the output signal with a stored password. More suitably, the comparison means further comprises means for outputting a signal dependent upon the correspondence of the output signal with the stored password.

Suitably, the input device comprises a keyboard.

Suitably, the set of available input signals comprises all or part of the character set of the keyboard.

Suitably, the system comprises a first input and a second input in which the character generator receives signals from the first input and does not receive signals from the second input.

Suitably, the first input is a local input device such as a keyboard or microphone and the second input is a remote based input device typically providing signals via a modem connection.

Suitably, the input signal comprises or corresponds to one of the set of input signals.

Suitably, the set of input signals comprises alphanumeric characters.

According to the present invention in a sixth aspect, there is provided a digital computer comprising a data communication system according to the fifth aspect of the invention.

According to the present invention in a seventh aspect, there is provided a data communication method comprising receiving an input signal available from a set of input signals, generating an output signal comprising a plurality of signals from the set of available input signals, in which the output signal is different from the input signal.

Suitably, the method further comprises the step of repeating the operation for a plurality of input signals.

Suitably, the output signals vary in length one from the other.

Suitably, the method according to the eighth aspect of the invention is modified according to the sixth aspect of the invention.

Brief Description of the Drawings

The present invention will now be described, by way of example only, with reference to the drawings that follow; in which:

Figure 1 is a schematic functional illustration of an embodiment of the present invention.

Figure 2 is a functional flow diagram illustrating operation of a preferred embodiment of the present invention.

Figure 3 is a diagram showing how data is stored according to the embodiment of the present invention described in relation to Figure 2.

Figure 4 is a functional flow diagram of the operation of the character generating device of the present invention in another embodiment.

Description of the Preferred Embodiments

Referring to Figure 1 of the drawings that follow, there is shown an electronic digital computer 2, typically a personal computer ("PC") comprising a keyboard 4 connected via a data line 6 to a processor 8. Those skilled in the art will appreciate that various elements intervene between the keyboard and processor.

On the data line 6 between keyboard 4 and processor 8 is a character generating device 10. The initials "CGD" are used for character generating device in this specification.

Other input ports 12, 14 as also shown which may for instance, be from a modem.

The character generating device 10 is configured to controllably modify the output of keystrokes from keyboard 4 to produce additional output for password verification, until that password verification is achieved and then revert to normal keyboard output operation.

The operation of the device will now be described in more detail with reference to Figures 2 onwards of the drawings that follow.

Upon activation of the application a password is requested to be input and the number of characters of an enhanced password is set. The input is "filtered" to recognise non-character codes such as CTRL and <SHIFT> so that these are not required in the user's password.

Referring now to Figure 2 of the drawings that follow, the keyboard 4, CGD 10 and a PC hard drive 16 are outlined. A user password (PW) is entered from keyboard 4. For purposes of explanation let the user password input be "BOB". The user sets the enhanced password length to, say, 10 characters. Upon an <ENTER> key strike (or typically for a WINDOWS (Registered Trade Mark) application, clicking the "OK" button) the user password BOB is enhanced.

Each CGD 10 contains a common key referred to as a NEPKEY. The CGD 10 uses a secret public key encryption algorithm with its own unique public key (the public key differs between CGD devices) to encrypt the NEPKEY, the result of which, referred to as Spk(NEPKEY) is stored on the PC hard drive. Thus the NEPKEY itself is not known outside of the CGD 10.

The CGD 10 creates a User Password Enchancer Encryption Key, referred to as UPEK, in a function called "GUPEK". A UPEK is generated in the CGD 10 as a random number. It need not be a random number, the main requirement being it is not known outside of the CGD 10. Each CGD 10 has the same NEPKEY (or set of NEPKEYs as several may be used), but a unique UPEK (or set thereof).

GUPEK is passed the Spk(NEPKEY) to be used to encrypt a new UPEK, how many new UPEK's are to within the set, and the location of the temporary resident program that can create UPEKs. It then passed the CGD 10 the encrypted

NEPKEY (ie T_{NEPKEY}(UPEK), where T is a symmetric encryption algorithm). As each new UPEK is created, according to the number to be generated, the CGD 10 encrypts it with the NEPKEY (ie T_{NEPKEY}(UPEK)). When it has finished, the temporary resident program is unloaded from the CGD 10. The CGD 10 then adds the encrypted UPEKs to one block of data, with a header 102 containing how many UPEKs 104a, 104b are within the set, as shown in Figure 3 of the drawings that follow. The NEPKEY encrypted UPEK is saved on the hard drive. Thus the UPEK is not known outside of the CGD 10. The generation of the Spk(NEPKEY) and T_{NEPKEY} (UPEK) are carried out in the set-up stage. There may be several UPEKs in a CGD 10.

At 100 the input user password is hashed to generate an output of predictable length, in this case 16 bytes. The primary reason for the HASH operation is to produce an irreversible result.

In the enhanced password generation method, at 106 the encrypted NEPKEY is retrieved from the PC hard drive 16 and decrypted by the CGD 10 to obtain the NEPKEY. Next at 108 the NEPKEY encrypted UPEK is retrieved and decrypted by the CGD 10 using the NEPKEY decrypted at 106 to obtain the UPEK.

The UPEK is encrypted by the HASH output from 100 and an enhanced password output of desired character length output. This enhanced password is stored, usually in the header portion of an application or document.

When access is sought to the application or document, the password enhancing application is activated and upon a user password being entered it is password enhanced as set out above, the result being compared with the password stored for the application or document. This comparison is carried out by the application itself, not by the CGD 10 that produces the enhanced password. As a modification the password checking can be carried out by the CGD 10 if it is loaded with appropriate software.

The CGD 10 is configured so that it will only accept one user password per second. The gap between acceptable inputs for password enhancing can be varied to provide additional security.

New NEPKEYs can be entered when required, preferably from a secure source so that the NEPKEY cannot be intercepted.

The HASH operation output length can be varied as a matter of design device. Normally it will be 64 to 128 bytes.

This system has several advantages as set out below:

(i) the user password is not stored on the PC so it cannot be retrieved by a hacker;

(ii) the relationship between the keyboard input and the CGD output (ie the enhanced password) is such that there is no practical reversibility;

(iii) by only permitting one password entry every second or so the system substantially prevents brute force attacks on the password. To succeed in a brute force attack a large number of permutations must be tried. At one entry per second the time required for a dictionary or brute force attack is unfeasible. For instance, at one million entries per second an six character password, with each character being selected from a possible 72 character set has 139,314,069,504 possible combinations that would take nearly 38 hours to try by brute force. If entry were restricted to one entry per second, the brute force attack would take 4417 years; and

(iv) because of the shared NEPKEY, hot seating (i.e. the use of different machines by one user) can be accommodated even though the CGD 10 on each machine has a different public key. The UPEK('s) associated with the particular user can be transferred securely between machines by encoding using the NEPKEY as a key ie T_{NEPKEY} (UPEK). It is noted that neither the NEPKEY(s) nor the UPEK(s) are seen or inspectable in plain (ie unencrypted) text outside of the secure CGD 10.

If desired new NEPKEYs can be downloaded into the CGD 10 using a security protocol.

A further embodiment of the present invention will now be described with reference to Figure 4 of the drawings that follow.

From a mode 200 in which the PC 2 is operating normally, an access is requested either to functions or data, the PC checks 202 to determine whether the function or data (say a file) is password protected. If not, the "NO" branch is followed and normal operation resumes with access permitted. If the function or data is password protected, the "YES" branch is followed and a suitable password is requested 204 and the character generating device is configured 206 to output additional characters according to a predetermined scheme.

Then, as each keystroke of the password is input 208 the signal is received by the device 10 and a corresponding longer output is generated 210. Thus, by way of example, if the keystroke "F" is entered, the device may output "P7TTWR0". The actual output is substantially immaterial so long as it is in accordance with a predetermined relationship between the input key and output sequence from the device 10.

The system then determines if the password input is finished 212. This may be by detecting the input of a <ENTER> key, the length of input or some other characteristic . If the input is not finished, the system requires a further input keystroke. If the input is finished, the "YES" branch is followed and the input password is compared with a password in memory 214. If the password is correct, the "YES" branch is followed, the character generator is configured 216 so input passes normally access to the function or data is permitted and normal operation resumed. If the password is incorrect, the "NO" branch is followed and access is denied 218.

Instead of access being denied on the first entry of an incorrect password, several attempts can be permitted, but normally not an unlimited number.

In addition to access being defined upon entry of incorrect password, additional alarm functions may be actuated.

The original password may also be input using this method and device. The user need never know or be concerned with the longer version of their password.

Accordingly, using the present invention it is possible for a user to remember a relatively short password, say "FRED" but for the processor to require validation of a much longer password which may or may not include the original password elements. By way of example, keyboard keystrokes of "FRED" at the password request stage may generate: P7aTWR0X3NR?B2aR88CI9CcAB.

So, a password input keystroke of four characters generates a twenty-six character long password for verification.

The device and system is configured so that remote access to the PC 2 is not via the device 10 so that such remote access requires entry of the full (longer) password required by the processor. Accordingly, protection from external hacking is enhanced.

The present invention can be embodied in hardware and/or software. Typically, in a hardware embodiment the device is located in a keyboard.

The "passwords" referred to herein may be of any signal or combination of signals and need not be "words" at all.

While the present embodiment has been described for use on a PC, it will be appreciated that the present invention can equally be put into effect on other platforms, devices or equipment.

The reader's attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.

All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive.

Each feature disclosed in this specification (including any accompanying claims, abstract and drawings), may be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a generic series of equivalent or similar features.

The invention is not restricted to the details of the foregoing embodiment(s). The invention extends to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel combination, of the steps of any method or process so disclosed.

Claims

1. A method for password enhancing, which method comprises the steps of entering a user password and irreversibly encrypting the user password.

2. A method according to claim 1, in which the encryption comprises a hash operation.

3. A method according to claim 1 or claim 2, in which the method comprises the additional step of using an encrypted first stored key (NEPKEY) to encrypt the irreversibly encrypted user password (HASH).

4. A method according to claim 3, in which the first stored key is encrypted by a public key encryption algorithm.

5. A method according to claim 3 or claim 4, in which the method comprises the additional step of decrypting an encrypted second stored key (UPEK) using the decrypted first stored key (NEPKEY).

6. A method according to claim 5, in which the second stored key is encrypted by a reversible algorithm.

7. A method according to claim 5 or claim 6, in which the result (HASH) of the irreversibly encrypted user password is encrypted using the second stored key (UPEK) as an encryption key.

8. A data access method comprising the steps of producing an enhanced password according to any one of claims 1 to 7,

comparing the enhanced password with a password associated with the data, and permitting access to the data only if the enhanced password and the data password correspond.

9. A computer program for carrying out the method of claim 8.

10. A carrier comprising a program according to claim 9.

11. A data communication system comprising an input device for generating a plurality of input signals available from a set of input signals and a character generator configured to receive an input signal and generate an output signal comprising a plurality of signals from the set of input signals in which the output signal is different from the signal input to the character generator.

12. A data communication system according to claim 11, in which the output signal is of a different length to the signal input to the character generator.

13. A data communication system according to claim 12, in which the output signal is longer than the signal input to the character generator.

14. A data communication system according to any one of claims 11 to 13, in which the system further comprises means for comparing the output signal with a stored password.

15. A data communication system according to claim 14, in which the comparison means further comprises means for

outputting a signal dependent upon the correspondence of the output signal with the stored password.

16. A data communication system according to any one of claims 11 to 15, in which the input device comprises a keyboard.

17. A data communication system according to claim 16, in which the set of available input signals comprises all or part of the character set of the keyboard.

18. A data communication system according to any one of claims 11 to 17, in which the system comprises a first input and a second input in which the character generator receives signals from the first input and does not receive signals from the second input.

19. A data communication system according to claim 18, in which the first input is a local input device such as a keyboard or microphone and the second input is a remote based input device typically providing signals via a modem connection.

20. A data communication system according to claim 19, in which the input signal comprises or corresponds to one of the set of input signals.

21. A data communication system according to claim 20, in which the set of input signals comprises alphanumeric characters.

22. A digital computer comprising a data communication system according to any one of claims 11 to 21.

23. A data communication method comprising receiving an input signal available from a set of input signals, generating an output signal comprising a plurality of signals from the set of available input signals, in which the output signal is different from the input signal.

24. A method according to claim 23, in which the method further comprises the step of repeating the operation for a plurality of input signals.

25. A method according to claim 23 or claim 24, in which the output signals vary in length one from the other.

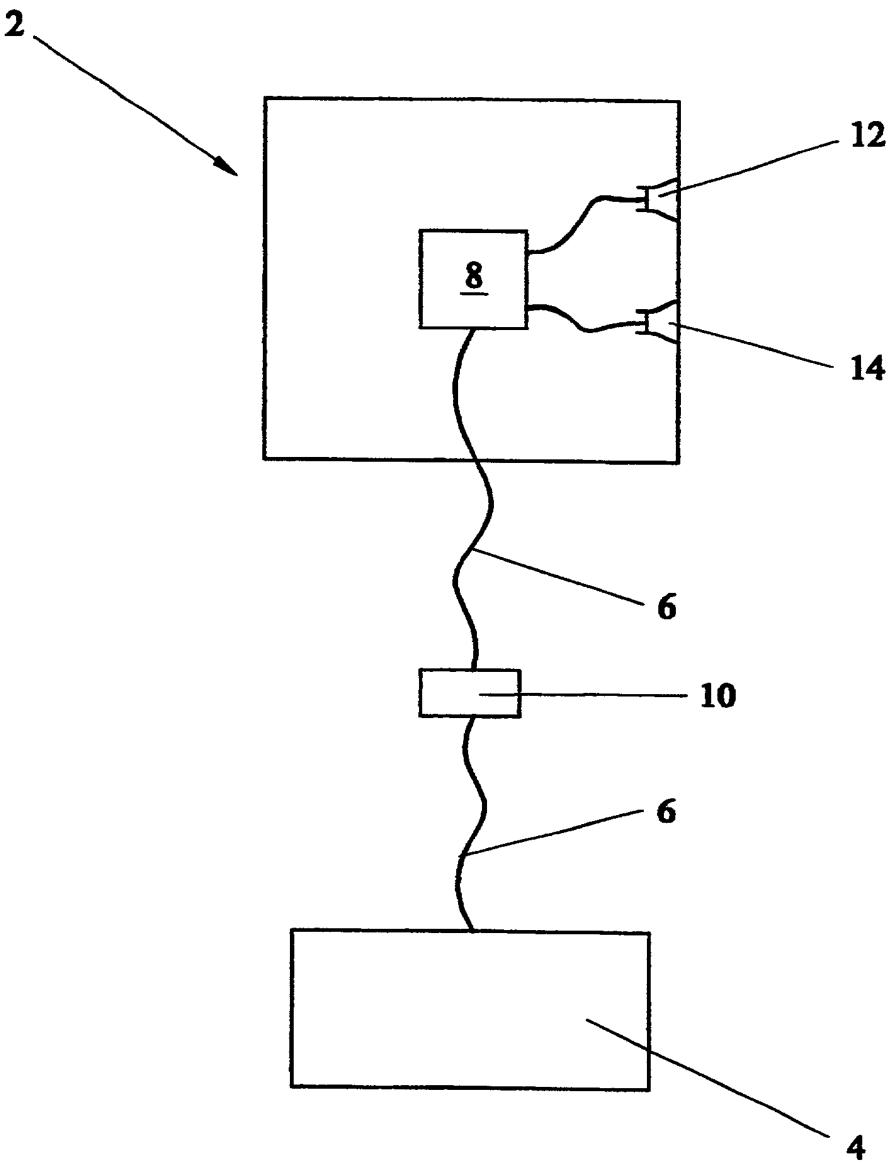

FIG. 1

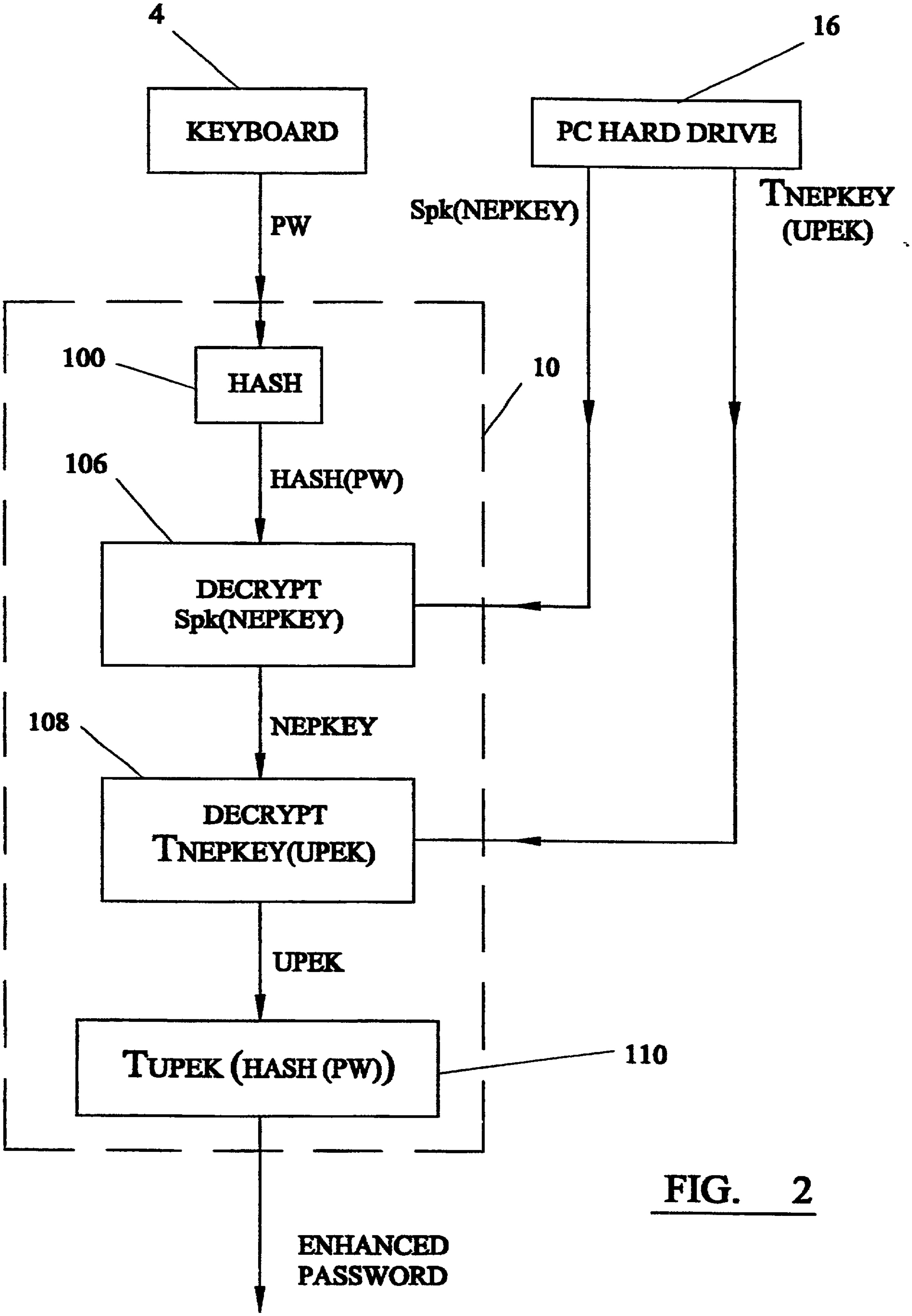
4
KEYBOARD
16
PC HARD DRIVE
PW
Spk(NEPKEY)
TNEPKEY
(UPEK)
100
HASH
10
106
HASH(PW)
DECRYPT
Spk(NEPKEY)
108
NEPKEY
DECRYPT
TNEPKEY(UPEK)
UPEK
TUPEK (HASH (PW))
110
ENHANCED
PASSWORD

FIG. 2

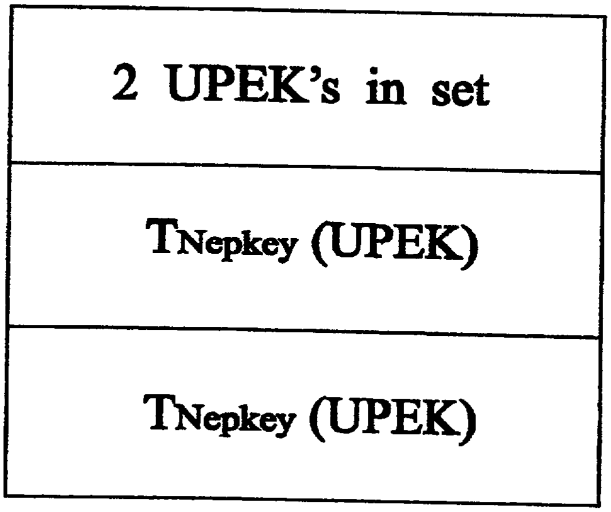

FIG. 3

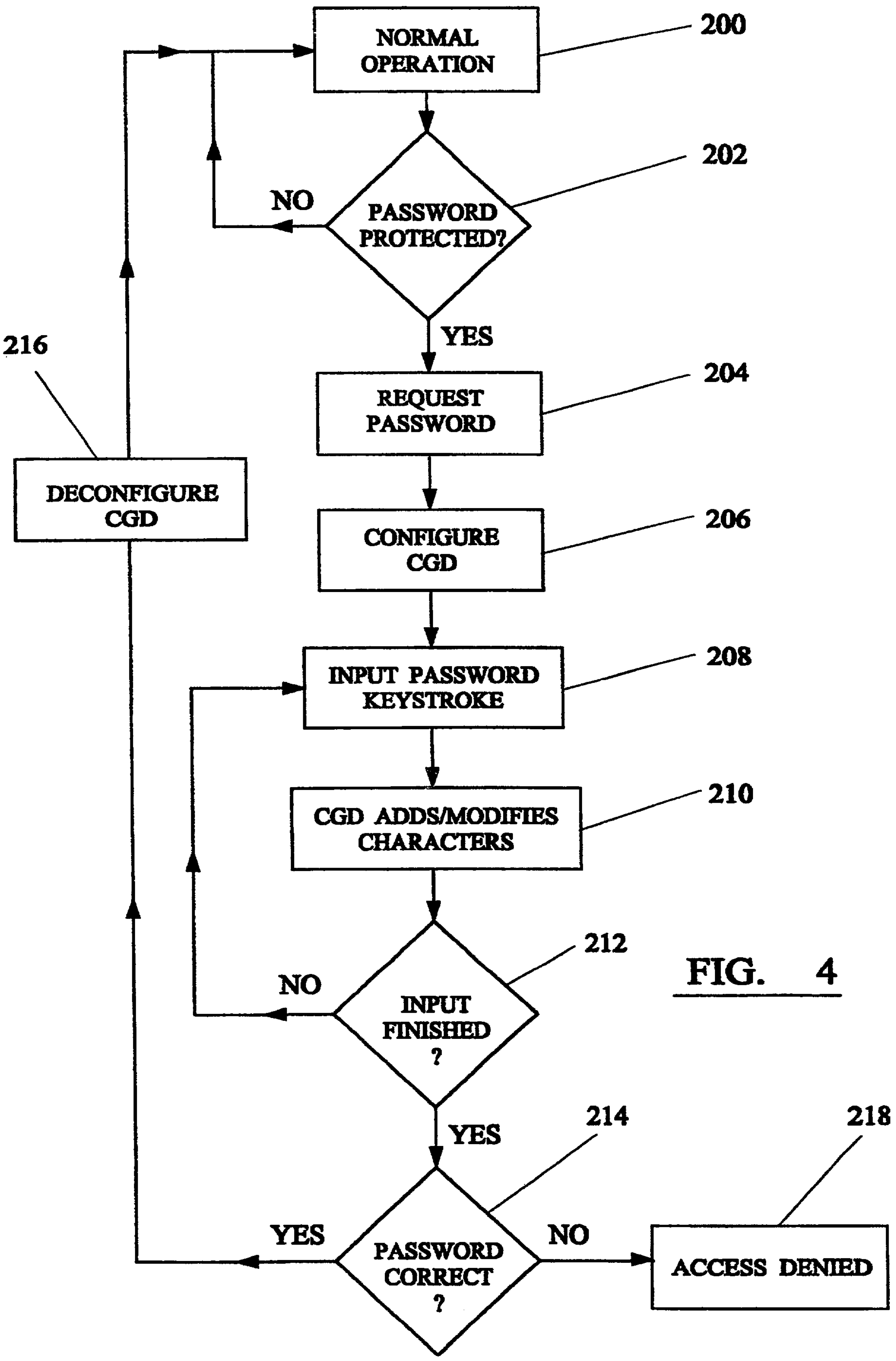
NORMAL OPERATION
200
PASSWORD PROTECTED?
202
NO
YES
REQUEST PASSWORD
204
CONFIGURE CGD
206
INPUT PASSWORD KEYSTROKE
208
CGD ADDS/MODIFIES CHARACTERS
210
INPUT FINISHED ?
212
NO
YES
PASSWORD CORRECT ?
214
YES
NO
ACCESS DENIED
218
DECONFIGURE CGD
216

FIG. 4

[illegible]

Declaration (37 CFR §1.63) for Utility or Design Application Using an Application Data Sheet (37 CFR §1.76) and Power of Attorney for Patent Application

As a below named inventor, I hereby declare that:

This declaration is directed to: IMPROVEMENTS IN AND RELATING TO DATA COMMUNICATION

[] The attached application, or

[✓] Application No. 09/763,103, filed on February 16, 2001
and was amended on ______ (if applicable);

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims, as amended by any amendment referred to above;

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

If this application is a continuation-in-part application, I acknowledge the duty to disclose to the Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56, which became available between the filing date of the prior application and the national or PCT international filing date of this continuation-in-part application.

I hereby declare that all statements made hereby of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

4

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agents(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: W. THAD ADAMS, III, REG. NO. 29,037; JEFFREY J. SCHWARTZ, REG. NO. 37,532; J. DEREL MONTEITH, JR., REG. NO. 46,464 and T. PEIGE WISE, REG. NO. 44,407 addressed to:

ADAMS, SCHWARTZ & EVANS, P.A.
2180 Two First Union Center
301 S. Tryon Street
Charlotte, North Carolina 28282
Telephone: 704-375-9249
Facsimile: 704-375-0729

I request that all correspondence, telephone calls and/or facsimiles be directed to W. Thad Adams, III, Jeffrey J. Schwartz, J. Derel Monteith, Jr. or T. Peige Wise at their above-stated address.

FULL NAME OF INVENTOR(S):

1 JK

Inventor one: Melih Abdulhayoglu Citizen of: Turkey

Signature: ______ Date: 2 APRIL 2001